EXHIBIT H

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventors:	Blayn W. Bennau, et al.	Atty.Dkt.No.:	6857-23201
Serial Number:	12/512,873	Examiner:	Reagan, James W.
Filing Date:	July 30, 2009	Group/Art Unit:	3621
Title:	METHODS, APPARATUS, AND COMPUTER PROGRAM PRODUCTS FOR SECURELY ACCESSING ACCOUNT DATA	Conf. No.	6515

******CERTIFICATE OF E-FILING TRANSMISSION******

I hereby certify that this correspondence is being transmitted via electronic filing to the United States Patent and Trademark Office on the date shown below:

On: March 2, 2015 (Date) /Paul T. Seegers/ Paul T. Seegers, # 66,621

RESPONSE TO FINAL OFFICE ACTION MAILED NOVEMBER 28, 2014

This paper is submitted in response to a Final Office Action of November 28, 2014, to further highlight why the application is in condition for allowance.

Please amend the case as listed below.

IN THE CLAIMS

The following is a current listing of claims and will replace all prior versions and listings of claims in the application. Please amend the claims as follows.

1. (Currently Amended) A method comprising:

~~receiving, by a computer-based system for securely downloading customer data to a browser toolbar and via the browser toolbar, a request for customer data from a customer;~~

detecting ~~determining~~, at a browser toolbar of a computer system ~~by the computer-based system~~, ~~that the~~ a request from a web service to obtain ~~for customer data includes a request for personal identifiable~~ account information of an account holder, wherein the account information is usable to conduct a transaction with the account holder ~~requiring encryption by a public encryption key generated by the browser toolbar~~;

~~authenticating, by the computer-based system, the customer based on a user credential and an account-specific access credential, wherein:~~

~~the user credential and the account-specific access credential are distinct, and~~

~~the account-specific access credential is associated with an account of the customer;~~

sending, by the browser toolbar, a request for the account information to a secure database that stores the account information;

decrypting ~~encrypting~~, by the browser toolbar ~~computer-based system~~, encrypted data received from the secure database, wherein the encrypted data includes the account information, wherein the decrypting is performed ~~the requested personal identifiable information~~ using ~~the public~~ an encryption key ~~generated~~ maintained by the browser toolbar and inaccessible outside of the browser toolbar; ~~and~~

securely storing the account information at the browser toolbar; and

removing the stored account information from the browser toolbar after completion of the transaction ~~transmitting, by the computer-based system, the encrypted personal identifiable information to the browser toolbar, wherein the encrypted personal identifiable information is decrypted by the browser toolbar and saved to a secure electronic wallet (e-wallet)~~.

2. (Currently Amended) The method of claim 1, ~~further comprising:~~ wherein the detecting includes analyzing, by the browser toolbar, content of the web service[[s]] to detect the request ~~initiated on a computer system executing the browser toolbar;~~

~~detecting, based at least in part on the analyzing, when the request for customer data includes the request for personal identifiable information; and~~

~~creating a public/private key pair combination in response to the detecting~~.

3. (Currently Amended) The method of claim 1, further comprising:

authenticating, via the browser tool, the account holder prior to sending the request for the account information ~~wherein the account specific access credential includes a card security code associated with the customer~~.

4. (Currently Amended) The method of claim 1, further comprising:

determining, by the browser toolbar ~~computer-based system~~, ~~that the~~ whether an account of the account holder ~~customer~~ is eligible ~~for use~~ to conduct a transaction with [[a]] the web service ~~initiating the request for customer data;~~

~~retrieving, by the computer-based system, generic account data associated with the account of the customer, wherein the generic account data includes information for the customer to decipher the account from another; and~~

~~transmitting, by the computer-based system, the generic account data to a computer system executing the browser toolbar~~.

5. (Currently Amended) The method of claim 1[[4]], wherein the removing is in response to closing a browser session with the web service ~~generic account data includes a portion of an account number associated with the account of the customer~~.

6. (Currently Amended) The method of claim 1[[4]], further comprising:

providing, via the browser toolbar, the stored account information to the web service in response to the detected request ~~receiving, via a user interface, a selection request indicating the customer requests access to personal identifiable information associated with the account of the customer; and~~

~~determining whether the customer has access to the personal identifiable information associated with the account of the customer based at least in part on the account specific access credential~~.

7. (Canceled)

8. (Currently Amended) A system, comprising:

a processor;

~~a tangible, non-transitory~~ memory ~~communicating with a processor for securely integrating personal identifiable information with a browser toolbar, the tangible, non-transitory memory~~ having instructions stored ~~thereon~~ therein that~~, in response to execution~~ are executable by the processor[[,]] to implement a browser toolbar that performs: ~~cause the processor to perform operations comprising:~~

~~receiving, by the processor, via the browser toolbar, a request for customer data from a customer;~~

identifying ~~determining, by the processor, that the~~ a request from a web service for account information associated with an account holder, wherein the account information is usable to conduct a transaction with the account holder ~~customer data includes a request for personal identifiable information requiring encryption with a public encryption key generated by the browser toolbar~~;

retrieving an encrypted version of the account information from a remote database;

~~authenticating, by the processor, the customer based on a user credential and an account specific access credential, wherein:~~

~~the user credential and the account specific access credential are distinct, and~~

~~the account specific access credential is associated with an account of the customer;~~

decrypting the encrypted version of the account information ~~encrypting, by the processor, the requested personal identifiable information~~ using ~~the public~~ an encryption key ~~generated~~ maintained by the browser toolbar; ~~and~~

completing a website form of the web service with a decrypted version of account information; and

deleting the decrypted version of the account information after completing the website form ~~transmitting, by the processor, the encrypted personal identifiable information to the browser toolbar, wherein the encrypted personal identifiable information is decrypted by the browser toolbar and saved to a secure electronic wallet (e-wallet)~~.

9. (Currently Amended) The system of claim 8, wherein the browser toolbar is further ~~configured~~ implemented to perform:

~~analyze web services initiated on a computer system executing the browser toolbar;~~

~~detect when the request for customer data includes the request for personal identifiable information; and~~

creating ~~create~~ a public/private key pair ~~combination~~, wherein the encryption key is a private key of the pair that is inaccessible outside of the browser toolbar; and

sending a public key of the pair to the remote database for encryption the account information.

10. (Currently Amended) The system of claim 8, wherein the account information ~~specific access credential~~ includes a card security code associated with an account of the account holder ~~the customer~~.

11. (Currently Amended) The system of claim 8, wherein the browser toolbar is further implemented to perform ~~comprising~~:

determining~~, by the processor, that~~ whether ~~the~~ an account of the account holder ~~customer~~ is eligible for use with [[a]] the web service ~~initiating the request for customer data;~~

~~retrieving, by the processor, generic account data associated with the account of the customer, wherein the generic account data includes information for the customer to decipher the account of the customer from another; and~~

~~transmitting, by the processor, via the transmission unit, the generic account data to a computer system executing the browser toolbar~~.

12. (Currently Amended) The system of claim 8[[11]], wherein the deleting is performed in response to termination of a browser session associated with the web service ~~generic account data includes a portion of an account number associated with the account of the customer~~.

13. (Currently Amended) The system of claim 8[[11]], wherein the deleting is performed in response to completion of the transaction ~~toolbar server application is further configured to:~~

~~receive, via a user interface, a selection request indicating the customer requests access to personal identifiable information associated with the account of the customer; and~~

~~determine whether the customer has access to the personal identifiable information associated with the account of the customer based at least in part on the account specific access credential~~.

14. (Currently Amended) A[[n]] ~~article of manufacture including a~~ non-transitory~~, tangible~~ computer readable medium having instructions stored thereon that~~, in response to execution~~ are executable by a ~~computer-based~~ computer system ~~for securely downloading customer data to a browser toolbar,~~ to cause the ~~computer-based~~ computer system to perform operations comprising:

~~receiving, by the computer-based system and via the browser toolbar, a request for customer data from a customer;~~

determining, at a browser toolbar, ~~by the computer-based system,~~ that [[the]] a request for account information has been received from a web service, wherein the account information is usable to conduct a transaction with an account holder ~~customer data includes a request for personal identifiable information requiring encryption by a public encryption key generated by the browser toolbar~~;

sending, via the browser toolbar, a request for the account information to a secure remote database; ~~authenticating, by the computer-based system, the customer based on a user credential and an account specific access credential, wherein:~~

~~the user credential and the account specific access credential are distinct, and~~

~~the account specific access credential is associated with an account of the customer;~~

decrypting, at the browser toolbar, encrypted data received from the remote database to obtain the account information, wherein the decrypting is performed ~~encrypting, by the computer-based system, the requested personal identifiable information~~ using ~~the public~~ an encryption key generated by the browser toolbar; ~~and~~

providing the account information to the web service to initiate the transaction; and

removing the account information from the computer system after providing the account information to the web service ~~transmitting, by the computer-based system, the encrypted personal identifiable information to the browser toolbar, wherein the encrypted personal identifiable information is decrypted by the browser toolbar and saved to a secure electronic wallet (e-wallet)~~.

15. (Currently Amended) The ~~article~~ computer readable medium of claim 14, ~~further comprising:~~ wherein the determining includes analyzing, by the browser toolbar, web service[[s]] content to detect the request from the web service ~~initiated on a computer system executing the browser toolbar;~~

~~detecting, by the browser toolbar, based at least in part on the analyzing, when the request for customer data includes the request for personal identifiable information; and~~

~~creating, by the browser toolbar, a public/private key pair combination in response to the detecting~~.

16. (Currently Amended) The ~~article~~ computer readable medium of claim 14, wherein the removing is performed in response to completion of the transaction ~~account specific access credential includes a card security code associated with the customer~~.

17. (Currently Amended) The ~~article~~ computer readable medium of claim 14, wherein the operations further ~~comprising~~ comprise:

generating the encryption key in response to the request from the web service; and

removing the encryption key from the computer system after the decrypting ~~determining, by the computer-based system, that the account of the customer is eligible for use with a web service initiating the request for customer data;~~

~~retrieving, by the computer-based system, generic account data associated with the account of the customer, wherein the generic account data includes information for the customer to decipher the account of the customer from another; and~~

~~transmitting, by the computer-based system, the generic account data to a computer system executing the browser toolbar~~.

18. (Currently Amended) The ~~article~~ computer readable medium of claim 17, wherein the encryption key is a private key having a corresponding public key ~~generic account data includes a portion of an account number associated with the account of the customer~~.

19. (Currently Amended) The ~~article~~ computer readable medium of claim 14, wherein the operations further comprise[[ing]]:

authenticating the account holder prior to sending the request to the secure remote database ~~receiving, by the computer-based system, via a user interface, a selection request indicating the customer requests access to personal identifiable information associated with the account of the customer; and~~

~~determining, by the computer-based system, whether the customer has access to the personal identifiable information associated with the account of the customer based at least in part on the account specific access credential~~.

20. (Canceled)

REMARKS

Claims 1-6 and 8-19 were pending in this application. Claims 1-6 and 8-19 have been amended. Claims 1-6 and 8-19 therefore remain pending in this application.

Examiner Interview

Applicant's undersigned representative and the Examiner conducted a telephone interview on January 23, 2015. The Examiner and Applicant's representative discussed amendments similar to those presented herein. Applicant's representative submitted arguments against the *Alice* rejections. The Examiner provided some helpful feedback. No formal agreement was reached, however. Applicant thanks the Examiner for his courtesy in conducting the interview. Applicant's remarks below reflect the substance of the interview.

Section 101 Rejections

All claims are rejected under 35 U.S.C. § 101 as being directed to abstract ideas in view of the Supreme Court Decision in *Alice Corporation Pty. Ltd. v. CLS Bank International, et al*. Office Action at 3-5. In support of this rejection, the Office Action states that "the invention is directed towards a method for encrypting and decrypting user personal data, which is the abstract idea of *(iv) a mathematical relationship or formula.*" Office Action at 5. The Office Action further asserts that "this amount[s] to no more than *(i) mere instructions to implement the idea on a computer.*" *Id.* Applicant respectfully disagrees.

As discussed in the interview, claim 1 has been amended to recite as follows:

1. A method comprising:
detecting, at a browser toolbar of a computer system, a request from a web service to obtain account information of an account holder, wherein the account information is usable to conduct a transaction with the account holder;
sending, by the browser toolbar, a request for the account information to a secure database that stores the account information;
decrypting, by the browser toolbar, encrypted data received from the secure database, wherein the encrypted data includes the account information, wherein the decrypting is performed using an encryption key maintained by the browser toolbar and inaccessible outside of the browser toolbar;
securely storing the account information at the browser toolbar; and
removing the stored account information from the browser toolbar after completion of the transaction.

In describing prior digital wallet solutions, Applicant's specification indicates that "[o]ne legitimate concern is that the information that is manually or automatically loaded at the customer's device can be exposed to rogue programs running on the customer's computing device." Specification at ¶ [0006]. The specification further discloses that, "[e]ven if the account data is ultimately stored in an encrypted form, the account data may also be exposed during data entry and prior to encryption by the digital wallet software." *Id.* The method recited in claim 1 attempts to overcome these deficiencies by providing a more secure way to handle account information. **First,** claim 1 recites "sending … a request for the account information to a secure database that stores the account information," "decrypting … encrypted data received from the secure database," and "removing the stored account information … after completion of [a] transaction." Accordingly, the account information is not manually entered into the computer system exposing it to a potential vulnerably; rather, the account information is "received from [a] secure database" as "encrypted data." Furthermore, the account information does not permanently reside at the computer system; rather, "the stored account information [is removed] … after completion of [a] transaction." **Second,** the actions recited in claim 1 are performed with respect to a "browser toolbar of a computer system," not some generic piece of software. **Third,** claim 1 recites "using an encryption key maintained by the browser toolbar and inaccessible outside of the browser toolbar." This stands in contrast to a digital wallet that might store encrypted data, but leave the key exposed. In sum, the recited method of claim 1 attempts improve the functioning of a computer system by providing a more secure way to manage critical information.

As a threshold matter, Applicant respectfully submits that claim 1 is not directed to the abstract idea of "a mathematical relationship or formula," Office Action at 5.[1] In *DDR Holdings*, the Federal Circuit held that the claims in question were not directed to a patent-ineligible abstract idea, in part, because the "asserted claims do not recite a mathematical algorithm." *DDR Holdings, LLC v. Hotels.com, L.P.*, __ F.3d __, sip op. at 19 (Fed. Cir. Dec. 5, 2014). In this instance, claim 1 also does not recite any mathematical relationship or formula.

Even assuming arguendo that claim 1's reference to decrypting encrypted data implies the use of some mathematical formula, it should be apparent from the discussion above that

[1] Claim 1 also does not recite "(i) a fundamental economic practice," "(ii) a method of organizing human activities," or "(iii) an idea of itself" (*See* Office Action at 3).

claim 1 recites substantially more than decrypting data. What is claimed is in fact a technical solution to a technical problem particular to data security with respect the Internet, and results in a considerable improvement to existing technology in this area for at least the three features of claim 1 noted above with respect to prior digital wallet implementations. Notably, the 2014 Interim Guidance on Patent Subject Matter Eligibility indicates that "[i]mprovements to the functioning of the computer itself" qualify as a judicial exception. *See* 79 FR 74624 (Dec. 16, 2014) (citing to *Alice Corp.,* 134 S. Ct. at 2359). Like the claims in *DDR Holdings,* the present claims "do not merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet," *DDR Holdings* at 20. Instead, "the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks," *id.* Again, claim 1 recites various operations performed via a "browser toolbar" to protect "account information." Thus, to the extent the present claims relate to some abstract idea, the claims recite substantially more than an abstract idea.

***

Applicant therefore respectfully requests withdrawal of the Section 101 rejections of all claims.

CONCLUSION:

Applicant respectfully submits the application is in condition for allowance, and an early notice to that effect is requested.

It should also be noted that although arguments have been presented with respect to certain claims herein, the recited subject matter as well as various other subject matter and/or combinations of subject matter may be patentable for other reasons. Further, the failure to address any statement by the Examiner herein should not be interpreted as acquiescence or agreement with such statement. Applicant expressly reserves the right to set forth additional and/or alternative reasons for patentability and/or allowance with the present Application or in any other future proceeding, and to rebut any statement presented by the Examiner in this or other papers during prosecution of the present Application.

If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above-referenced application from becoming abandoned, Applicant hereby petitions for such extension.

The Commissioner is authorized to charge any fees that may be required, or credit any overpayment, to Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C. Deposit Account No. 501505/6857-23201/PTS.

Also filed herewith is the following item:

☒ Request for Continued Examination

Respectfully submitted,

Date: March 2, 2015

By: /Paul T. Seegers/
Paul T. Seegers
Reg. No. 66,621

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P. O. Box 398
Austin, Texas 78767
(512) 853-8878